IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

| | | |
|---|---|---|
| IN THE MATTER OF THE SEARCH OF: | ) | |
| | ) | Case No. 1:23-sw-5 |
| [redacted] | ) | **UNDER SEAL** |
| ASHBURN, VIRGINIA 20147 | ) | |

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE**

I, Brandy Oliva, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as [redacted], Ashburn, VA 20147, hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent of the U.S. Department of Homeland Security, Homeland Security Investigations ("HSI"), and I have been so employed since 2017. I am currently assigned to the Child Exploitation Group in Reston, Virginia. Previously, I was a child protective services investigator for the state of Texas where I specialized in child abuse investigations.

3. While employed by HSI, I have investigated federal criminal violations related to child exploitation and child pornography as well as narcotics smuggling and money laundering. I have gained experience through everyday work related to conducting these types of investigations. I also have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media.

Due to my experience and training, I can identify child pornography when I see it. Moreover, I am a federal law enforcement officer who is engaged in enforcing criminal laws, including 18 U.S.C. §§ 2251, 2252 and 2252A, and I am authorized by law to request a search warrant.

4. The facts and information in this affidavit are based upon information that I obtained during this investigation and information that has been provided to me by other law enforcement sources. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

## RELEVANT STATUTES AND LEGAL DEFINITIONS

6. Based upon my training, experience, and discussions with federal prosecutors that I have worked with on this and other similar investigations, I have learned that:

a. 18 U.S.C. § 2252(a)(2)/(b)(1) prohibits any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed, or that has been shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproducing or attempting to reproduce any visual depiction for distribution using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce or through the mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

b. 18 U.S.C. § 2252(a)(4)(b)/(b)(2) prohibits any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, one or more books, magazines, periodicals, films, video tapes, or other matter

which contain any visual depiction that has been mailed, or that has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

## DEFINITIONS

7. The following definitions apply to this Affidavit and Attachment B:

a. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.

b. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

c. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, flash drives or thumb drives, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices,

mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

d. A "wireless telephone," or mobile or cellular telephone, is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

e. A "tablet" is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "Wi-Fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

f. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and

other magnetic or optical media.

g. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

h. "Wireless routers" create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

i. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer or other digital device to access the Internet. IP addresses can be "dynamic," meaning that the Internet service provider ("ISP") assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static" if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

j. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

k. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

l. "Records," "documents," and "materials," as used herein, include all information recorded in any form and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

m. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

**n.** "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

## BITTORRENT FILE SHARING NETWORK

5. Peer-to-Peer (P2P) file sharing is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the

network. These P2P networks are commonly referred to as decentralized networks because each user of the network is able to distribute information and queries directly through other users of the network, rather than relying on a central server to act as an indexing agent, where all of the information is first deposited before it is distributed. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up files on a computer to be shared with others running compatible P2P software. However, only files that are specifically stored in shared folders are exchanged. Therefore, a user needs simply to move a file from one folder to another to stop the distribution across the Internet. Further, once a file or files are placed in a shared folder, its distribution is dependent only on the machine being turned on, the file sharing software being initiated, and the computer being connected to the Internet.

8. BitTorrent is one type of P2P file sharing software. Users of the BitTorrent network wishing to share new content will use a BitTorrent program to create a "torrent" file for the file or group of files they wish to share. A torrent file is a small file that contains information about the file(s) and provides a method for a user to download the file(s) referenced in the torrent from other BitTorrent users. Torrent files are typically found as the result of keyword searches on Internet sites that host or link to them. Torrent files may be referenced by their "infohash," which uniquely identifies the torrent based on the file(s) associated with the torrent file. To download file(s) from other users on the BitTorrent network, a user typically obtains a torrent file. The BitTorrent software processes the information in the torrent file and locates devices on the BitTorrent network sharing all or parts of the actual file(s) being sought. The download of the content referenced in the torrent is achieved after the requesting computer and the sharing computer(s) directly connect to each other through the Internet using the BitTorrent software.

9. The BitTorrent network bases all of its file shares on the Secure Hash Algorithm (SHA-1). This mathematical algorithm allows for the digital fingerprinting of data. A torrent file is not the actual digital content but, instead, it defines the files to be shared as a series of contiguous pieces. The SHA-1 hash value for each "piece" of the torrent file is contained within the torrent file, as well as filenames, file sizes, and other data. Once you check a file or files with a SHA-1 hashing utility capable of generating this SHA-1 value (the fingerprint), that will be a fixed-length unique identifier for that file or files. The SHA-1 hash is the current Federal Information Processing and Digital Signature Algorithm. The SHA-1 is secure because it is computationally infeasible for two files with different content to have the same SHA-1 hash value.

10. Once a needed piece is downloaded via the BitTorrent network, the SHA-1 hash value of that piece is checked against the value within the torrent file. As soon as a piece is downloaded and verified, the software makes that piece available to upload to other peers who need and request it. This means that a user can share pieces of a file before they have the entire collection of files designated by the torrent file. Basically, a user can share the pieces they have if they do not have every piece identified by the torrent file.

11. One of the advantages of P2P file sharing is that multiple files may be downloaded at the same time. In addition, a user may download pieces of one file from more than one source computer at a time. For example, a BitTorrent user downloading a movie file may actually receive pieces of the movie from multiple computers. The advantage of this is that it speeds up the time it takes to download the file. It is possible to also download the file or files from only one computer.

12. A P2P file transfer is assisted by reference to an Internet Protocol ("IP") address. This address is unique to a particular computer during an online session. The IP address provides a unique location making it possible for data to be transferred between computers.

## STATEMENT OF PROBABLE CAUSE

13. On or about July 13, 2022, Special Agent Daniel Schneider used a BitTorrent application in Fairfax, Virginia to conduct an undercover investigation into the Internet distribution and possession of child pornography. During this investigation, a device sharing suspected child pornography was located on the BitTorrent file sharing network. Special Agent Schneider made a direct connection to the device assigned the IP address [redacted] (hereinafter "TARGET IP") and downloaded files associated with the torrent info hash [redacted]. Special Agent Schneider downloaded files from the TARGET IP at 22:45:27 EDT on July 13, 2022. There were two folders located within this torrent -- one named "[redacted]" and one named "[redacted]." I reviewed the image files that were downloaded from the TARGET IP and contained in both file folders. Through my training and experience, I determined that there were image files contained in these file folders that apparently depicted child pornography. The following is a representative sample and description of a few of the image files that Special Agent Schneider downloaded from the TARGET IP:

a. File Folder: [redacted]

File Name: [redacted]

SHA1 HASH VALUE: [redacted]

File Description: This video is approximately 35 minutes and 41 seconds in length. Special Agent Schneider downloaded approximately 1 minute and 15 seconds of the video. [redacted]

[redacted]

b. File Folder: [redacted]

File Name : [redacted]

SHA1 HASH VALUE: [redacted]

File Description: The video is approximately 19 seconds in length. [redacted]

c. File Folder: [redacted]

File Name: [redacted]

SHA1 HASH VALUE: [redacted]

File Description: This is a partially downloaded video approximately 46 seconds long. [redacted].

14. On or about July 14, 2022, Special Agent Schneider used a BitTorrent application in Fairfax, Virginia to conduct an undercover investigation into the Internet distribution and possession of child pornography. During this investigation, a device sharing suspected child

pornography was located on the BitTorrent file sharing network. Special Agent Schneider made a direct connection to the device assigned the TARGET IP and downloaded files associated with the torrent info hash [redacted]. Special Agent Schneider downloaded files from the TARGET IP at 15:19:11 EDT on July 14, 2022. I reviewed the files that were downloaded by Special Agent Schneider. The main file folder was named "[redacted]." The following is a representative sample and description of one of the files Special Agent Schneider downloaded from the TARGET IP:

a. File Name: [redacted]

SHA1 HASH VALUE: [redacted]

File Description: The video is approximately 7 minutes and 40 seconds in length. [redacted]

15. On or about October 16, 2022, Virginia State Police Special Agent Michael Sponheimer used a BitTorrent application in Fairfax, Virginia to conduct an undercover investigation into the Internet distribution and possession of child pornography. During his investigation, a device sharing suspected child pornography was located on the BitTorrent file sharing network. Special Agent Sponheimer made a direct connection to the TARGET IP and downloaded files associated with the torrent info hash [redacted]. Special Agent Sponheimer downloaded files from the TARGET IP at 00:27:21 EDT on October 16, 2022. I reviewed the files that were

downloaded by Special Agent Sponheimer. Below provides a description of the content/subject matter of one of the downloaded files:

a. File Name [redacted]

SHA1 VALUE: [redacted]

File Description: The video is approximately 14 minutes and 30 seconds in length. [redacted]

16. On or about July 15, 2022, Special Agent Schneider served an administrative summons to Verizon. The summons requested subscriber information associated with the TARGET IP on July 13, 2022, at 21:50 EST, the date and time of the downloads described in Paragraph 13. On July 28, 2022, Verizon returned the following information pursuant to the above-described summons:

Customer Name: [redacted]

Account Address: [redacted], Ashburn, VA 20147 (the PREMISES)

IP Address: [redacted]

Subscriber Phone Number: [redacted]

Email Address: [redacted]

17. On or about August 24, 2022, Special Agent Schneider served an administrative summons to Verizon. The summons requested the current IP address for [redacted], Ashburn, VA 201417. On September 2, 2022, the Verizon return listed [redacted] as

an active IP address for [redacted], Ashburn, VA 201417 from March 2022 to August 2022.

18. On or about December 7, 2022, a query on [redacted] in a Department of Homeland Security maintained database was conducted. This query revealed that [redacted] is a United States citizen and married to a Louis Eugene Staudenmaier, who is also a United States citizen. [redacted] Virginia driver's license issued in 2019 lists her residential address as the PREMISES. Additionally, Louis Eugene Staudenmaier's Virginia driver's license issued in 2019 also lists the PREMISES as his residential address.

19. In or about December 2022, I conducted a query via an open-source database. According to information contained in this database, both Staudenmaiers are associated with the PREMISES.

20. From September 2022 to December 2022, periodic surveillance was conducted at the PREMISES. The vehicles observed in the driveway of the home on multiple occasions included a black Audi sedan with Virginia license plate [redacted] and a white Audi SUV with Virginia license plate [redacted]. According to law enforcement database checks conducted on or about December 7, 2022, Louis Staudenmaier is the registered owner of the black Audi sedan and [redacted] is the registered owner of the white Audi SUV. Both vehicles also list the PREMISES on their registration.

21. In or about December 2022, an Internet search for the property records of the PREMISES revealed the owners as Louis and [redacted] Staudenmaier.

22. On or about December 2022, a query on the PREMISES in a Department of Homeland Security maintained database was conducted. The search revealed an additional possible resident of the PREMISES as [redacted], brother of [redacted]. [redacted]

[redacted] is a United States citizen and possibly employed by ARK Systems Inc. based out of Columbia, Maryland. [redacted] Maryland driver's license issued in September 2016 lists an additional possible residence in Frederick, Maryland.

23. According to photos posted on a publicly-available Facebook page with the name [redacted] maiden name) in late 2022, [redacted] is the mother of two children believed to be infant/toddler age.

## CHARACTERISTICS OF CHILD PORNOGRAPHERS

24. Individuals who have a sexual interest in children or images/videos of children almost always possess and maintain child pornographic material. These individuals may collect sexually explicit or suggestive materials depicting children in a variety of media including, but not limited to, digital media, photographs, motion picture films, magazines, negatives, correspondence, books, drawings, slides, and magnetic media. These images/videos are usually maintained in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain such images/videos for many years.

25. Individuals who have a sexual interest in children or images/videos of children rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

26. Individuals who have a sexual interest in children or images/videos of children often delete child pornography material after downloading or viewing it online. However, when a person "deletes" data stored on a digital storage device, the data does not actually disappear;

rather, that data remains on the digital storage device until it is overwritten by new data. Using forensic tools, "deleted" data can be recovered months or even years later.

27. Individuals whose sexual interest in children or images/videos of children has led them to purchase access to membership, subscription-based websites, or other commercial sources of child pornography frequently maintain the financial records of those transactions at their residences.

28. Based on the information provided in this affidavit, I believe that an individual residing at the PREMISES likely displays characteristics common to individuals who receive, possess, or access with intent to view child pornography. As stated above, it is believed an individual utilizing the TARGET IP accessed the BitTorrent network to receive files consistent with child pornography.

**COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

29. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41€(2)(B).

30. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files

downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

31. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the

PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating

or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., Internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how

computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, pieces, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is dynamic. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

32. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data

on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

33. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

## BIOMETRIC UNLOCKING

34. *Unlocking the device(s) with biometric features*. The warrant I am applying for would permit law enforcement to compel certain individuals to unlock a device subject to seizure pursuant to this warrant using the device's biometric features. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris

recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data

based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted

Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the Subject Premises and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

35. Due to the foregoing, if law enforcement personnel encounter a device that is subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) depress the occupant's thumb and/or fingers onto the fingerprint sensor of the digital device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of the occupant's face with his or her eyes open to activate the facial, iris, or retina-recognition feature, for the purpose of attempting to

unlock the device in order search the contents as authorized by this warrant.

## CONCLUSION

36. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,

BRANDY D OLIVA

Digitally signed by BRANDY D OLIVA
Date: 2023.01.06 10:40:28 -05'00'

Special Agent Brandy Oliva
Homeland Security Investigations

SWORN AND SUBSCRIBED BEFORE ME THIS 6TH DAY OF JANUARY, 2023.

Lindsey Vaala

Digitally signed by Lindsey Vaala
Date: 2023.01.06 11:39:56 -05'00'

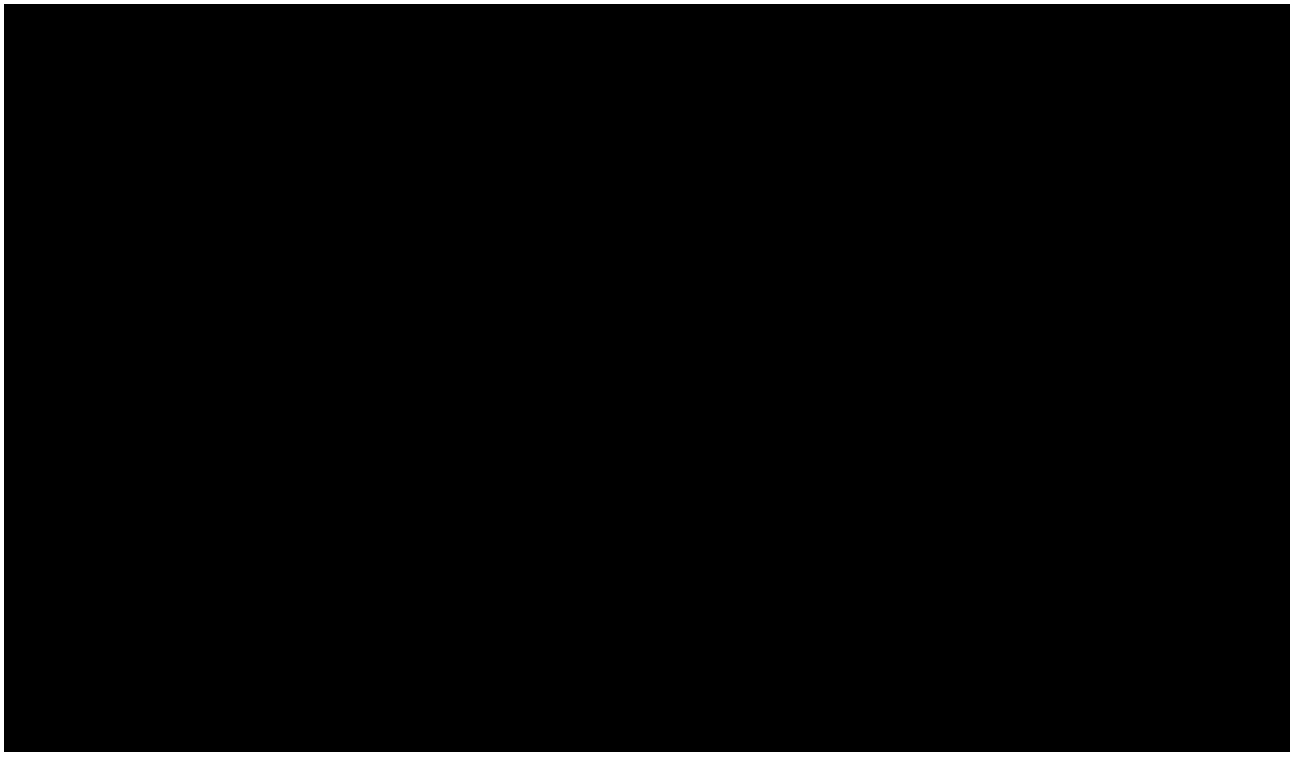
Honorable Lindsey R. Vaala
United States Magistrate Judge
Alexandria, Virginia

**ATTACHMENT A**

*Property to be searched*

The property to be searched is [redacted], Ashburn, VA 20147. This is a two-story red brick house with dark shutters flanking the windows located on approximately one acre of land. A plaque with the numbers "[redacted]" is affixed on a post at the entrance of the driveway of the home.

The following is a photograph of the outside of the PREMISES:



## ATTACHMENT B

*Property to be seized*

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. §§ 2252(a)(2) and (a)(4)(B):

1. Computers or storage media owned, possessed, used, or otherwise associated to Tamar Staudenmaier and/or Louis Eugene Staudenmaier, which were used as a means to commit the violations described above.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chats," instant messaging logs, photographs, and correspondence;

b. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. Evidence of the lack of such malicious software;

d. Evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

e. Evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;

f. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. Evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. Evidence of the times the COMPUTER was used;

i. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. Records of or information about Internet Protocol addresses used by the COMPUTER;

l. Records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. Contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet;
4. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES including utility and telephone bills, mail envelopes, or addressed correspondence.

5. Child pornography and child erotica.

6. Records, information, and items relating to violations of the statutes described above including:

a. Records, information, and items relating to the occupancy or ownership the PREMISES, including utility and telephone bills, mail envelopes, or addressed correspondence;

b. Records, information, and items relating to the ownership or use of the computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;

c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;

d. Records and information relating to the sexual exploitation of children;

e. Records and information showing access to and/or use of BitTorrent and related peer-to-peer networks;

f. Records and information relating or pertaining to the identity of the person or persons using or associated with BitTorrent;

g. Written or typed passwords, passcodes, or encryption keys that would be necessary to access data on computers, storage devices or electronic equipment described above;

h. Records and information written or typed that describe or document the violator's sexual interest in children.

During the execution of the search warrant, law enforcement is permitted to: (1) depress the occupant's thumb and/or fingers onto the fingerprint sensor of the digital device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be

depressed; and (2) hold the device in front of the occupant's face with his or her eyes open to activate the facial, iris, or retina-recognition feature, for the purpose of attempting to unlock the device in order search the contents as authorized by this warrant.

Law enforcement is not authorized to require anyone to disclose a password or identify specific biometric characteristics that may be used to unlock the device, including which finger or other physical features unlock the device, in order to gain access to the contents of the device. Nor does the warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain display of any biometric characteristics to compel an occupant to state or otherwise provide that information. However, the voluntary disclosure of such information by an occupant is permitted. To avoid confusion on that point, if agents in executing the warrant ask an occupant for the password to any device(s), or to identify which biometric characteristic unlocks any device, the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

As used above, the terms "records" and "information" include all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD and macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, CDs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.